



Kaspersky Industrial  
Cybersecurity  
Conference 2023

# Обновления KICS

Стрелков Андрей

Руководитель направления развития продуктов для промышленной безопасности



kaspersky

# Содержание

1. Основные направления развития платформы KICS
2. Минорные обновления
3. Интеграция KICS и SD-WAN
4. Обновления ICS TI

# Основные направления развития

2023

## **OT XDR**

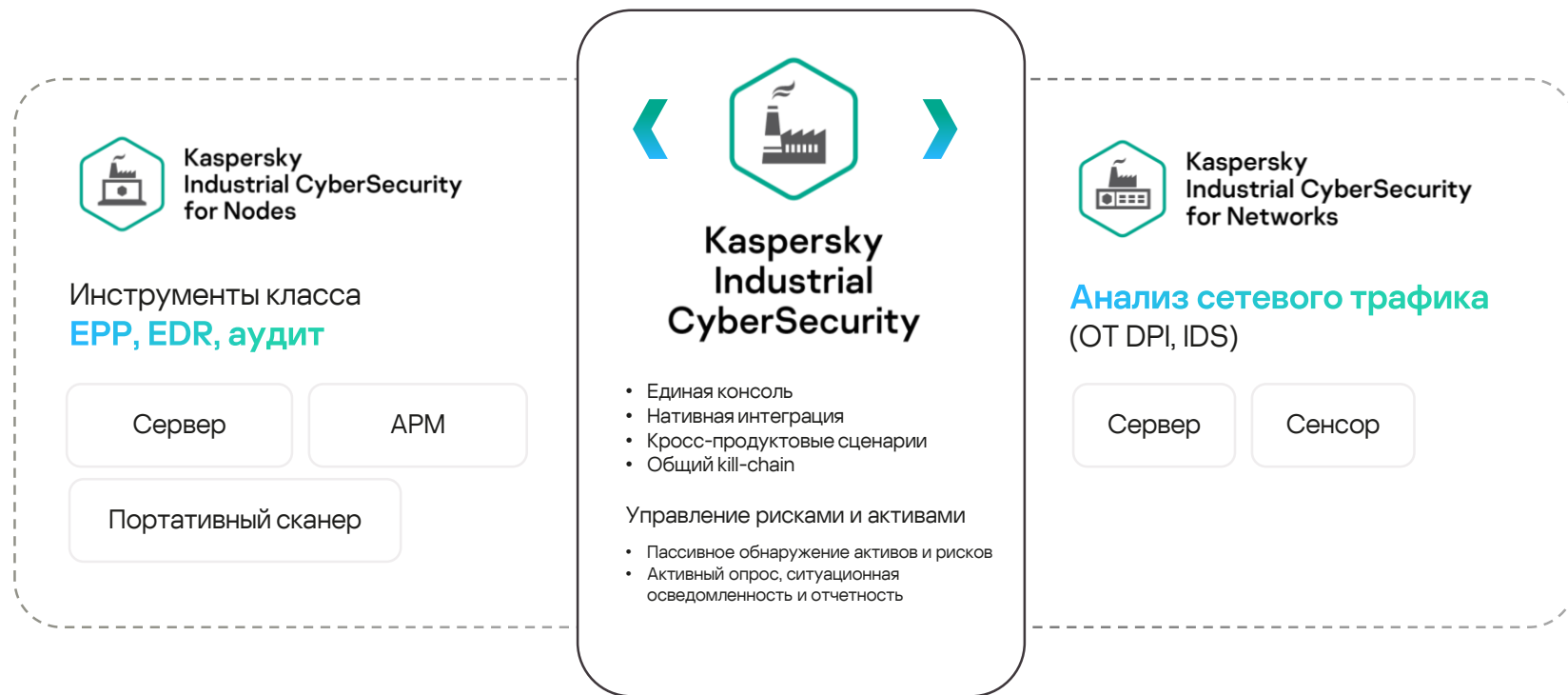
Платформа для расширенного детектирования и реагирования на угрозы для промышленных сред

## **Аудит безопасности**

Централизованная система для аудита безопасности узлов промышленной сети

## **NTA**

Комплексный анализ сетевого трафика



# Нативная\* система для расширенного детектирования и реагирования на угрозы

\* Нативная – значит состоящая только из продуктов ЛК:  
KICS for Nodes + KICS for Networks

## **Для OT сегмента**

Подходит для изолированных промышленных сетей и для команд ИБ АСУ ТП

## **Только базовые решения**

Сетевой и узловой сенсоры.  
Управление на сервере KICS for Networks, не нужно дополнительное оборудование или лицензии



События и инциденты Действия по реагированию

## События и инциденты

Изменить статус Показать связи Загрузить трафик Коллировать детали

# Карточка сетевого детекта

- Детали актива
- Описание события
- Информация о приложении
- Список IoC

## 9.6 Обнаружено несоответствие (SEQUENCE ABNORMAL MULTIPLE COMMAND) X

Изменить статус Показать связи Реагирование на угрозы Создать разрешающее правило Загрузить трафик

## Возможные последствия

- Отключение устройств.
- Изменение конфигураций устройств.
- Изменение параметров технологического процесса.

## Меры по устранению угроз

- Определить инцидатора события по адресной информации (IP-адрес, MAC-адрес) и отключить от сети при несанкционированном подключении или несоответствии требуемым функциям.
- Проверить работу сетевого оборудования и средств защиты информации и при необходимости изменить параметры.
- Если событие зарегистрировано в результате замены оборудования и новое оборудование разрешено для использования, создайте разрешающее правило по технологии Контроль системных команд.

## Приложение

Поставщик	Siemens AG, PTD EA
Название	RC-PCSW-CFE
Версия	2.22.13
Путь	C:\Program Files (x86)\Siemens Energy\SiCAM\PAS PQS\CFE\Bin\CfeIEC104Slave.exe
Операционная система	Microsoft Windows 7
Адрес стороны взаимодействия	172.17.0.235:49432
Является сервером	Нет
Подпись	Недействительная
MD5	<a href="#">d1daf7170987525fe2aec0c4d7926c08_?</a>
SHA256	<a href="#">b6900bd74df374e5f966bd727426d642e3feb1e21e8a098d0691308904dc41cc_?</a>

## Пользователь приложения

Имя	SiCAM-PAS\PASRuntimeUser
Тип учетной записи	Не администратор
Тип входа	Прокси

## Приложение

Поставщик	—
Название	—
Версия	—
Путь	C:\Users\Demo\AppData\Local\Temp\Industroyer_104_kit\starter.exe
Операционная система	Microsoft Windows Server 2012 R2 Standard
Адрес стороны взаимодействия	172.17.0.235:49432
Является сервером	Нет
Подпись	Недействительная
MD5	<a href="#">c93c8d4ea47ee7d68f4830333e94e388_?</a>
SHA256	<a href="#">edfff8ab0bb74cb2957a02a978f2ff31a96cba78f6643701cb949bce4e36672_?</a>

## Пользователь приложения

Имя	RDC\RDC\$
Тип учетной записи	Не администратор
Тип входа	Не определен

# Карточка EDR-детекта:

- Детали актива
- Описание события
- Цепочка атаки на узле
- Список IoC
- Реагирование

### 8.4. Обнаружен зараженный или возможно зараженный объект

0 событий | **Группы событий активности** | Все события активности

```

graph TD
    A[C:\Users\Demo...\starter.exe] --> B[Создание файла 3]
    B --> C[C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe]
    C --> D[C:\Users\Demo\AppData\Local\Temp\Industroyer_104_kit\104.dll]
  
```

#### Информация об обнаружении

<b>Файл</b>	
Дата и время	08.09.2023 15:36:23
Имя	C:\Users\Demo\AppData\Local\Temp\Industroyer_104_kit\104.dll
Размер	134 КБ
Хеш MD5	<a href="#">66c67ebf254f29bf925a8ae6a3163a1c</a>
Хеш SHA256	<a href="#">b60f097b12087f2d809d4d4f945a9fe2e372fbae67a0e483237a2ced9d99b27e5</a>
Создан	08.09.2023 15:36:22
Изменен	08.09.2023 15:36:22
Атрибуты	Архивный
Подписавшая организация	—
Доверенная цифровая подпись	Нет
Создатель	NT AUTHORITY\SYSTEM
Идентификатор часового пояса	Компьютер

<b>Данные о загрузке</b>	<b>Данные о модификации</b>
Веб-адрес загрузки	Хеш MD5 программы
Загружившая программа	Хеш SHA256 программы
Хеш MD5 программы	
Хеш SHA256	

# Анализ трафика внутри периметра инфраструктуры объекта

Разбирает как промышленные, так и корпоративные протоколы

## **Отображение сессий**

Список всех сетевых сессий с детальной информацией для расследования инцидентов

## **Сохранение трафика и загрузка PCAP**

Сохранение «сырого» трафика для последующего анализа

Новый модуль для поиска статистических аномалий и атак в сетевом трафике (брутфорс, спуфинг)

Карта сетевых взаимодействий    Топологическая карта    Сетевые сессии

## Карта сетевых взаимодействий

Настроить виды    Настроить группы    Загрузить трафик    Изменить статус    Показать связи    Объединить устройства    Фильтр по событиям

Статусы устройств    Оценки соединений    Протоколы    Состояния устройств    Категории устройств    Уровни модели OSI

Все статусы    Все оценки    Все протоколы    Все состояния    Все категории    Все уровни     Связанные устройства

+ 66% -

**Соединение**

Показать связи

Уровень важности: Средний (4 - 7.9)

**HACKER-ENGINEER**

Статус: **Неразрешенное**

Адресная информация: Сетевой интерфейс 1  
00:0c:29:01:51:e9  
172.17.0.227

↓

**RDC**

Статус: **Разрешенное**

Адресная информация: Intel(R) 82574L Gigabit Network Connection  
00:0c:29:51:40:12  
172.17.0.235  
и еще 1 IP-адрес и 1 сетевой интерфейс

**Протоколы**

TCP	2 КБ
SMB	1 КБ

**Коммуникация на карте сети:**

- Данные об активах
- Адресная информация

# Новая вкладка – Список сетевых сессий

Карта сетевых взаимодействий | Топологическая карта | **Сетевые сессии**

### Сетевые сессии

[Показать связи](#) | [Загрузить трафик](#) | [Экспорт в CSV-файл](#)

ID устройств: **30** x | [Фильтр по умолчанию](#)

<input type="checkbox"/>	Статус	Сторона 1	Порт с...	Сторона 2	Порт с...	Устройство 1	Устройство 2	Протокол пере...	Прот...
<input type="checkbox"/>	Заверш...	00:0c:29:015f...	1524	00:0c:29:5140...	135	HACKER-ENGINEER	RDC	TCP	DCE/RPC
<input checked="" type="checkbox"/>	Заверш...	00:0c:29:015f...	1523	00:0c:29:5140...	445	HACKER-ENGINEER	RDC	TCP	SMB
<input type="checkbox"/>	Заверш...	00:0c:29:015f...	1525	00:0c:29:5140...	49157	HACKER-ENGINEER	RDC	TCP	TCP
<input type="checkbox"/>	Заверш...	00:0c:29:5140...	0	00:0c:29:015f...	0	RDC	HACKER-ENGINEER	Ethernet II	ARP
<input type="checkbox"/>	Заверш...	00:0c:29:015f...	1520	00:0c:29:5140...	445	HACKER-ENGINEER	RDC	TCP	SMB
<input type="checkbox"/>	Заверш...	00:0c:29:015f...	1522	00:0c:29:5140...	49157	HACKER-ENGINEER	RDC	TCP	TCP
<input type="checkbox"/>	Заверш...	00:0c:29:015f...	1521	00:0c:29:5140...	135	HACKER-ENGINEER	RDC	TCP	DCE/RPC
<input type="checkbox"/>	Заверш...	00:0c:29:015f...	1513	00:0c:29:5140...	445	HACKER-ENGINEER	RDC	TCP	SMB
<input type="checkbox"/>	Заверш...	00:0c:29:015f...	1514	00:0c:29:5140...	135	HACKER-ENGINEER	RDC	TCP	DCE/RPC
<input type="checkbox"/>	Заверш...	00:0c:29:5140...	0	00:0c:29:015f...	0	RDC	HACKER-ENGINEER	Ethernet II	ARP
<input type="checkbox"/>	Заверш...	00:0c:29:015f...	1515	00:0c:29:5140...	49157	HACKER-ENGINEER	RDC	TCP	TCP

### 172.17.0.227 → 172.17.0.235

[Показать связи](#) | [Загрузить трафик](#) | [Экспорт в CSV-файл](#)

Статус:  Завершена

Протокол передачи: TCP

Протокол приложений: SMB

Текущая скорость: 0 бит/с

Средняя скорость: 26 кбит/с

Всего передано: 236 КБ

Точки мониторинга: mp1

Начало: 08.09.2023 15:36:09

Последнее взаимодействие: 08.09.2023 15:37:23

Количество пакетов: 388

#### Сторона 1

Устройство: **HACKER-ENGINEER**

Адрес: 172.17.0.227

Порт: 1523

↓

#### Сторона 2

Устройство: **RDC**

Адрес: 172.17.0.235

Порт: 445

Карта сетевых взаимодействий | Топологическая карта | Сетевые сессии

**Сетевые сессии**

Показать связи | Загрузить график | Экспорт в CSV-файл

Статус	Сторона 1	Порт с...	Сторона 2	Порт с...	Устройство 1	Устройство 2	Протокол пере...	Прот...
Заверш...	00:0c:29:01:51...	1523	00:0c:29:51:40...	445	HACKER-ENGINEER	RDC	TCP	SMB
Заверш...	00:0c:29:01:51...	1525	00:0c:29:51:40...	49157	HACKER-ENGINEER	RDC	TCP	TCP
Заверш...	00:0c:29:51:40...	0	00:0c:29:01:51...		RDC	HACKER-ENGINEER	Ethernet II	ARP
Заверш...	00:0c:29:01:51...	1520	00:0c:29:51:40...	445	HACKER-ENGINEER	RDC	TCP	SMB
Заверш...	00:0c:29:01:51...	1522	00:0c:29:51:40...	49157	HACKER-ENGINEER	RDC	TCP	TCP
Заверш...	00:0c:29:01:51...	1521	00:0c:29:51:40...	135	HACKER-ENGINEER	RDC	TCP	DCE/RPC
Заверш...	00:0c:29:01:51...	1513	00:0c:29:51:40...	445	HACKER-ENGINEER	RDC	TCP	SMB
Заверш...	00:0c:29:01:51...	1514	00:0c:29:51:40...	135	HACKER-ENGINEER	RDC	TCP	DCE/RPC
Заверш...	00:0c:29:51:40...	0	00:0c:29:01:51...	0	RDC	HACKER-ENGINEER	Ethernet II	ARP
Заверш...	00:0c:29:01:51...	1515	00:0c:29:51:40...	49157	HACKER-ENGINEER	RDC	TCP	TCP

## Список сессий:

- Полная информация о всех сессиях в рамках коммуникации
- Статус сессии
- Данные об активах
- Адресная информация, порты
- Протоколы
- Объем переданных данных/текущая скорость сессии
- Время начала и окончания

Карта сетевых взаимодействий | Топологическая карта | Сетевые сессии

## Сетевые сессии

Показать связи | Загрузить трафик | Экспорт в CSV-файл

Фильтры

30 x Фильтр по умолчанию

Статус	Сторона 1	Порт	Сторона 2	Порт	Устройство 1	Устройство 2	Протокол	Проп.
Заверш.	00:00:29:01:51:1524	1524	00:00:29:01:51:1523	1523	HACKER-ENGINEER	RDC	TCP	DCE/D
Заверш.	00:00:29:01:51:1525	1525	00:00:29:01:51:1522	1522	HACKER-ENGINEER	RDC	TCP	TCP
Заверш.	00:00:29:01:51:40	0	00:00:29:01:51:40	0	HACKER-ENGINEER	HACKER-ENGINEER	Ethernet II	ARP
Заверш.	00:00:29:01:51:1520	1520	00:00:29:01:40:448	448	HACKER-ENGINEER	RDC	TCP	SMB
Заверш.	00:00:29:01:51:1522	1522	00:00:29:01:51:1522	1522	HACKER-ENGINEER	RDC	TCP	TCP
Заверш.	00:00:29:01:51:1521	1521	00:00:29:01:51:1521	1521	HACKER-ENGINEER	RDC	TCP	TCP
Заверш.	00:00:29:01:51:1513	1513	00:00:29:01:51:1513	1513	HACKER-ENGINEER	RDC	TCP	SMB
Заверш.	00:00:29:01:51:1514	1514	00:00:29:01:51:1514	1514	HACKER-ENGINEER	RDC	TCP	DCE/D
Заверш.	00:00:29:01:51:40	0	00:00:29:01:51:40	0	HACKER-ENGINEER	HACKER-ENGINEER	Ethernet II	ARP
Заверш.	00:00:29:01:51:1515	1515	00:00:29:01:40:49157	49157	HACKER-ENGINEER	RDC	TCP	TCP

## Карточка сессии:

- Детальная информация о выбранной сессии
- Переходы на карточки активов
- Возможность загрузить PCAP-дамп выбранной сессии

172.17.0.227 - 172.17.0.235

Показать связи | Загрузить трафик | Экспорт в CSV-файл

Протокол передачи	TCP
Протокол приложений	SMB
Текущая скорость	0 бит/с
Средняя скорость	26 кбит/с
Всего передано	236 КБ
Точки мониторинга	mp1
Начало	08.09.2023 15:36:09
Последнее взаимодействие	08.09.2023 15:37:23
Количество пакетов	388

Сторона 1

Устройство **HACKER-ENGINEER**

Адрес 172.17.0.227

Порт 1523

↓

Сторона 2

Устройство **RDC**

Адрес 172.17.0.235

Порт 445

Карта сетевых взаимодействий    Топологическая карта    Сетевые сессии

### Карта сетевых взаимодействий

Настроить виды    Настроить группы    Загрузить трафик    Изменить статус    Показать связи    Объединить устройства    Фильтр по событиям

Статусы устройств    Оценки соединений    Категории устройств    Уровни модели OSI  
 Все статусы    Все оценки    Все протоколы    Все состояния    Все категории    Все уровни    Связанные устройства

+ 66%    [Иконка]

**Возможность получить PCAP-дамп всего трафика**

#### Соединение

Показать связи

Уровень важности: Средний (4 - 7.9)

**HACKER-ENGINEER**  
 Статус: **Неразрешенное**  
 Адресная информация: Сетевой интерфейс 1  
 00:0c:29:01:51:e9  
 172.17.0.227

↓

**RDC**  
 Статус: **Разрешенное**  
 Адресная информация: Intel(R) 82574L Gigabit Network Connection  
 00:0c:29:51:40:12  
 172.17.0.235  
 и еще 1 IP-адрес и 1 сетевой интерфейс

**Протоколы**  
 TCP    2 KB  
 SMB    1 KB

08.09.23 16:35

## Загрузка трафика:

- Авто-сбор со всех Сенсоров и точек мониторинга за заданный период
- Внутреннее «встроенное» хранилище
- Внешнее подключаемое хранилище для больших объемов данных или длительного периода хранения
- Фильтрация пакетов с помощью BPF как для сохранения, так и для загрузки трафика

### Загрузка трафика

Внутреннее хранилище	Внешнее хранилище
Самый старый пакет 01.01.1970 03:00:00	Статус хранилища Не подключено

Период для загружаемого трафика

08.09.2023 15:35:45 - 08.09.2023 15:36:45

Максимальный объем для загрузки

Макс. объем 100 Ед. изм. МБ

Фильтрация по точкам мониторинга

Включить фильтрацию

Точки мониторинга Точки мониторинга не выбраны

Фильтрация с использованием BPF

Включить фильтрацию

Выражение для фильтрации (пример: top port 102 or top port 502)

host172.17.0.235

Фильтрация с использованием регулярных выражений

Включить фильтрацию

Выражение для фильтрации (пример: \*test.+xABxCD)

Не задано

Загрузить Отмена

# Аудит безопасности

## Ключевые преимущества

Аудит безопасности для узлов на Windows, Linux и сетевого оборудования

Открытый язык описаний Open Vulnerability and Assessment Language (OVAL)

Полнофункциональный редактор для проверок и параметров безопасности

Встроенная база уязвимостей для промышленного ПО от Kaspersky ICS CERT

Задачи для одного узла или групповые, запускаемые вручную или по расписанию

Поддержка сторонних и пользовательских баз OVAL

Отчёты, результаты аудита и история проверок доступны в одном месте

Защищённое хранилище секретов для безагентского аудита



# Опрос устройств для аудита



Kaspersky  
Industrial  
CyberSecurity

SSH

## Безагентский

Linux рабочие станции и  
серверы, сетевое  
оборудование

Требуется учетная запись

KICS for Nodes

## Через Агент

Windows рабочие станции и  
серверы  
(Linux в 2024)

Не требуется учетная запись

Наборы правил    Задания

### Наборы правил аудита безопасности

Импорт    Удалить    + Добавить задание

<input type="checkbox"/> Имя ↓	Изменено	Источник
<input type="checkbox"/> База данных уязвимостей Kaspersky ICS CERT для АСУ ТП	08.09.2023	Система
<input type="checkbox"/> БДУ ФСТЭК	08.09.2023 13:15:26	Пользователь
<input type="checkbox"/> Общие настройки безопасности Astra Linux SE и CE	08.09.2023 13:09:37	Система
<input type="checkbox"/> Общие настройки безопасности Debian	08.09.2023 13:09:37	Система
<input type="checkbox"/> Общие настройки безопасности Red Hat Enterprise Linux, CentOS, Oracle Linux	08.09.2023 13:09:37	Система
<input type="checkbox"/> Общие настройки безопасности SUSE Linux Enterprise, openSUSE	08.09.2023	Система
<input type="checkbox"/> Общие настройки безопасности Ubuntu	08.09.2023	Система
<input type="checkbox"/> Общие настройки безопасности Windows 10	08.09.2023	Система
<input type="checkbox"/> Общие настройки безопасности Windows 11	08.09.2023	Система
<input type="checkbox"/> Общие настройки безопасности Windows 7	08.09.2023	Система
<input type="checkbox"/> Общие настройки безопасности Windows 8.1	08.09.2023 13:09:37	Система
<input type="checkbox"/> Общие настройки безопасности Windows Server 2012	08.09.2023 13:09:37	Система

Наборы правил содержат инструкции для задачи аудита для определенных типов узлов, ПО или стандартов.

Выбор встроенной конфигурации безопасности или пользовательского правила

Выбор правил

Выбор устройств

Настройка задания

Выбор правил

Набор правил

Общие настройки безопасности Astra Linux SE и CE

Профиль

По умолчанию

Важно...	Класс
<input checked="" type="checkbox"/>	Введение
<input checked="" type="checkbox"/>	Системные настройки
<input checked="" type="checkbox"/>	Установка и обслуживание ПО
<input type="checkbox"/>	Права доступа к файлам и маски
<input type="checkbox"/>	Ограничение параметров монтирования разделов
<input type="checkbox"/>	Ограничения динамического монтирования и отключения фа...
<input type="checkbox"/>	Проверка прав доступа у важных файлов и директорий
<input type="checkbox"/>	Ограничение программ от возможного опасного поведен...
<input checked="" type="checkbox"/>	Учётные записи и контроль доступа
<input checked="" type="checkbox"/>	Настройка сети и брандмауэра
<input checked="" type="checkbox"/>	Настройка Syslog

Правила описывают настройки системы, снижающие ее безопасность, и их целевое состояние.

Возможность задания кастомизированного профиля для аудита

## Настройка задания

Имя задания

Задание Аудита Astra Linux

Описание

Проверка по расписанию Astra

Способ опроса

Удаленное подключение ▾

Подключение с узла

KICS4NET41 ▾

Секрет с учетными данными

Linux ▾



Регистировать обнаруженные уязвимости

### Расписание

Запускать задание по расписанию

Периодичность

Каждый месяц ▾

Время запуска (UTC)

16:19

Запускать каждый

1 ▾

день месяца

### Отчеты

Отправлять по электронной почте

Адреса получателей

+ Добавить

Задания для аудита  
можно настраивать  
централизованно для  
всех сегментов с  
сенсорами KICS for  
Networks

Возможность опрашивать  
устройства по расписанию  
и отправлять отчеты по  
почте

## Общие сведения

### Сведения о задании аудита безопасности

Генератор OVAL: Общие настройки безопасности Astra Linux SE и CE  
 Дата и время генерации набора: 02.11.2022 17:14:59      Количество правил в задании: 109  
 Количество правил в наборе: 109      Метод сканирования: Удаленное сканирование

### Общие р

✖ Есть

### По пр

Соотв

Несоо

Други

Правило	Важность
✖ Директория /var/log располагается на отдельном разделе	Низкая
✖ Директория /home располагается на отдельном разделе	Низкая
✖ Права доступа к файлам и маски	
✔ Ограничение параметров монтирования разделов	
✔ Добавление noexec, nosuid опции для съемных носителей	Низкая
✔ Добавление опции noexec для /home и /tmp разделов	Низкая
✖ Проверка прав доступа у важных файлов и директорий	
✖ Проверка прав доступа у файлов, содержащих информацию о локальных учётных записях	
✖ Ограничить права на crontab файл	Средняя

После выполнения  
формируется pdf-  
отчет

Отчет содержит  
сводку и результаты  
проверок

По всем  
несоответствиям  
инструкция по  
устранению

ID определения: oval.ru.atlx-soft.nixdef:26069      Важность: Средняя

Имя правила: Ограничить права на crontab файл

Описание: Системные файлы crontab доступны только демону cron (с привилегиями суперпользователя) и команде crontab (запускаемая от root). Если непривилегированным пользователям дать права на чтение или (что ещё хуже) модификацию системных crontab файлы, то это может привести к повышению привилегий локального пользователя. Для правильного задания прав и группы, необходимо выполнить команды: # chmod 400 /etc/crontab # chmod -R 770 /var/spool/cron/ # chown -R 0 /var/spool/cron/

# Минорные обновления

2023

Гранулярные настройки  
обучения KICS for Networks

Улучшения UI KICS for Networks

Улучшения KICS for Nodes

**KICS-WINSRV2016**

Изменить | Изменить статус | Показать связи | Выполнить

Состояние безопасности: **OK** | Категория: KICS-W | Сетевое имя: KICS-W | Группа: -

Значимость: **Высокая**

Статус: Разрешенное

Общие | Адреса | Параметры контроля процесса | Параметры топологии | Оборудование

Процессоры: Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz (1 ядро), 1 логический процессор  
 BIOS: VMware, Inc. 255.255.24.12.2020  
 ОЗУ: 4 ГБ  
 Локальные диски: C: свободно 70 из 89 ГБ  
 Оптические приводы: NECVMWar VMware SATA CD00

USB-устройства

- Generic USB Hub
  - Значение PNPClass: USB
  - Значение DeviceID: USB\VID\_0E0F&PID\_0002\6&201153C1&0&7
- Generic USB Hub
  - Значение PNPClass: USB
  - Значение DeviceID: USB\VID\_0E0F&PID\_0002\6&201153C1&0&8
- USB Input Device
  - Значение PNPClass: HIDClass
  - Значение DeviceID: USB\VID\_0E0F&PID\_0003&MI\_00\7&2A0405E8&0&0000

В режиме наблюдения не обновляется адресная информация для устройств со ста...

Создано: 08.09.2023 12:57:33  
 Последнее изменение: 08.09.2023 13:00:24  
 Последнее появление: 11.09.2023 23:53:42

Адресная информация

Intel(R) 82574L Gigabit Network Connection

MAC-адрес: 00:0c:29:9c:60:89  
 IP-адрес: 192.168.5.24

Показать адреса всех сетевых интерфейсов (3)

Аппаратное обеспечение

Производитель: VMware, Inc.  
 Модель: VMware7,1  
 Версия: VMware7,1

ОС: Windows Server 2016  
 Маршрутизирующее устройство: Нет  
 ID устройства: 5  
 Риски: **Небезопасная архитектура сети**

Программное обеспечение

**KICS-WINSRV2016**

Изменить | Изменить статус | Показать связи | Выполнить

Состояние безопасности: **OK** | Сетевое имя: KICS-W | Группа: -

Значимость: **Высокая**

Изолировать устройство от сети | Отключить сетевую изоляцию | Реагирование на угрозы | Параметры топологии | Параметры контроля процесса | Настроить группы

Подключение Kaspersky Endpoint Agent: **Активное**  
 Последнее: 11.09.2023 23:55:32

Оптимизация пространства, больше информации в карточке

Данные в карточке разбиты по секциям

Множество инструментов для работы с событиями и устройствами

## KICS4NET41-SENSOR1 ×

[Изменить](#) [Удалить](#) [Выключить все](#) ⋮  **Наследовать технологии Сервера**

[Управление технологиями](#) [Параметры](#)

[Включить все](#) [Выключить все](#) Режим **Смешанный** ▾

<input checked="" type="checkbox"/> <b>AM</b> Обнаружение активности устройств	<b>Наблюдение</b> ▾	
<input checked="" type="checkbox"/> <b>CC</b> Контроль системных команд	<b>Обучение</b> ▾	<b>до: 29.09.2023 00:11</b>
<input checked="" type="checkbox"/> <b>DPI</b> Контроль процесса по правилам	<b>Обучение</b> ▾	<b>до: 29.09.2023 00:11</b>
<input checked="" type="checkbox"/> <b>NIC</b> Контроль целостности сети	<b>Обучение</b> ▾	<b>до: 06.10.2023 00:11</b>
<input checked="" type="checkbox"/> <b>AM</b> Контроль проектов ПЛК		
<input checked="" type="checkbox"/> <b>AM</b> Обнаружение сведений об устройствах		
<input type="checkbox"/> <b>DPI</b> Обнаружение неизвестных тегов		
<input type="checkbox"/> <b>DPI</b> Обнаружение устройств для контроля процесса		

Сенсоры и точки мониторинга могут наследовать настройки сервера или иметь свои

Удобно подключать новые площадки – пока вся система в режиме мониторинга, новая площадка может обучаться

Таймер на обучение – автоматическое переключение в режим мониторинга

# Обновления продукта KICS for Nodes

## Улучшения Firewall Management

- Гибкое управление уровнем интеграции
- Сканирование исходящего трафика
- Фильтрация по диапазону портов
- Разрешающие и запрещающие правила

Поддержка новых моделей ПЛК в модуле PLC Integrity Control: Siemens S7-1500, Prosoft Regul, ARIS, EKRA

Сертификация модуля контроля устройств (DC) и сертификация по МЭК 62443-4-1

# Интеграция KICS и SD-WAN

2023

Мониторинг географически  
распределенных инфраструктур –  
множество необслуживаемых или  
обслуживаемых небольших  
площадок.

# Решение: интеграция KICS и SD-WAN

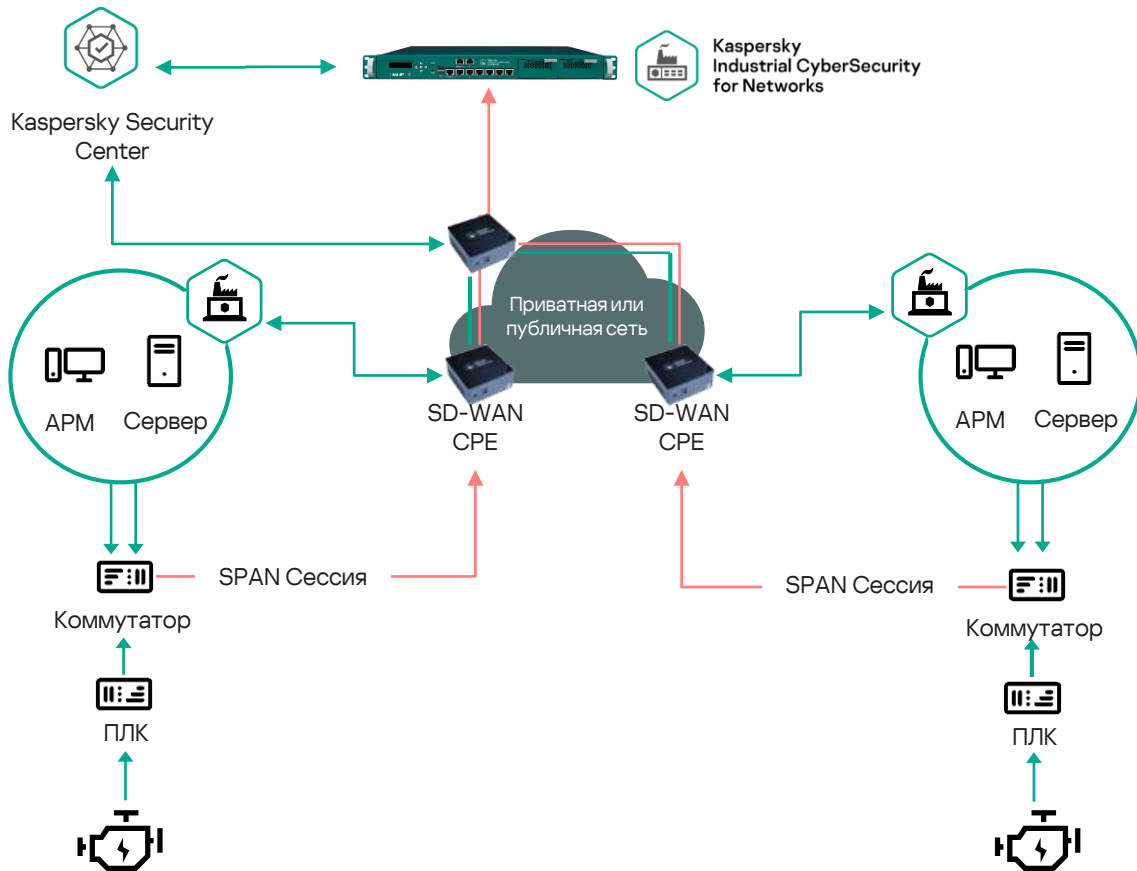
Возможность передачи  
SPAN-сессии напрямую с  
удаленного объекта на  
сервер/сенсор в HQ.

Масштабируемая  
транспортная сеть, через  
разные технологии доступа с  
дублированием каналов

Гибкая и легкая в настройке SD-  
WAN, есть компактное CPE

«Встроенный» мониторинг  
промышленного трафика!

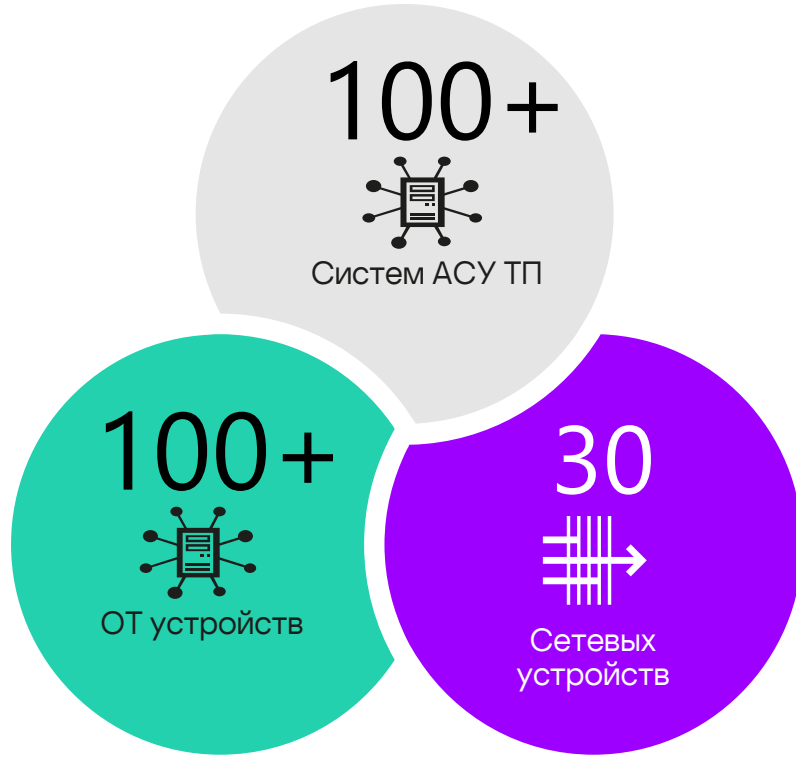
# Интеграция KICS for Networks и Kaspersky SD-WAN



- Гибкость в создании распределённой инфраструктуры ИБ
- Компактное портативное устройство CPE, не требует много места
- SPAN-трафик передается на сервер или сенсор KICS for Networks в центральном офисе
- Разделение каналов внутри канала SD-WAN / поддержка различных сценариев, не влияющих друг на друга
- Поддержка резервирования через несколько каналов связи

# Обновления ICS TI

2023



- Пассивный анализ уязвимостей теперь поддерживает не только ПЛК, но и сетевые устройства  
Уже около 30 моделей поддержано
- Встроенные в KICS OVAL базы для детекта уязвимостей для более 100 различных АСУ ТП от более 20 вендоров (треть отечественных)
- Пассивный контроль целостности проекта ПЛК
- Импорт из SCADA проектов для устройств и тегов

# Спасибо!

Ждем вас на демо!

Стрелков Андрей

Руководитель направления развития  
продуктов для промышленной безопасности

Telegram: @dogsraspberries

**kaspersky**